Ameliorating the Performance of a Hybrid CMFD Technique

Saini Rakesh [1]
Research Scholar, Department of Computer Science,
JJT University, Jhunjhunu-Churu Road, Vidyanagari, Dist Jhunjhunu, Churela, Rajasthan, India

Singh Sanjay [2]
Scientist-C, IC Design Group
CSIR—Central Electronics Engineering Research Institute (CSIR-CEERI), Pilani, Rajasthan, India

Abstract

In this paper the hybrid image forgery detection algorithm is proposed. The method presented in this paper is a copy-move forgery detection, which is often observed in digital pictures. Digital image processing is applied to images which are digital in nature through digital data processors. Digital images are modified effortlessly using available software and advanced digital cameras. Any software program (e.g., Photoshop, 3DS Max, Coral Draw) creates image manipulation that it is really hard to distinguish tampered images from their actual counter parts. The sharing of a personal photo and album is very common in social media. Onlooker changes personal images and albums which create serious problems. Content tampering detection for digital snapshots is, thus, an essential research area. In that location are numerous types of tampering, specifically composting, morphing, re-touching, enhancement, PC generated, and painting. The copy-move forgery detection of 48 high resolution .png images is detected. The algorithm comparison is performed using different parameters like precision, recall and f1 value with state of the art techniques. The experimental results achieved average precision 98%, recall 100% and f1 99% average accuracy.

Keywords: Scale-Invariant Feature Transform (SIFT), copy move forgery (CMF), Simple Linear Iterative Clustering (SLICO), Singular Value Decomposition (SVD), discrete wavelet transform (DWT).

INTRODUCTION

The rapid boom of image processing software and the advancement in digital cameras have turned over the upward trend of forged image with no apparent traces. Image forgery has a long story. Today's digital world, it is workable to create and change the records represented via a photograph very effortlessly, without leaving any apparent traces of these operations. In recent years blind digital image forgery detection discipline has given away a great interest from the scientific community. Existing digital photo forensics techniques can be categorized into active and passive (blind) schemes.

Active techniques work only in the presence of some prior statistics about the icon [1]. In passive approaches, additionally recognized as blind techniques, the source image is unavailable. There is no such need of any priori records of the photo as in active techniques. The most simple of all the attacks is copy move forgery (CMF), which involves the duplication of a certain location (or regions) within the image. Reproduction of image areas is, sometimes, accomplished from other digital images as in picture splicing. The passive photograph forgery detection algorithms can be grouped majorly under five categories, i.e., pixel based, camera based, and compression based, geometric based and physics based systems. CMF is the most frequent case of picture forgery which involves copying and pasting of a certain character in the same digital picture. The replicated segments can be made to persist one or a compounding of some geometrical transformations such as rotation, scaling, and hence along. To find an image forgery number of basic steps is performed such as:

Image Pre-Processing and Statistical Analysis

Before any function extraction procedure, some of the methods are accomplished over a verification image, which include resizing, cropping, grayscale conversion from RGB shade space etc. for the classification overall performance improvement.

Feature Extraction and Selection

The feature band is pressed out for each class which is beneficial in telling it from all the different classes, in the mean time being in reality invariant to all the variations in attributes inside a classification of the host tampered data.

Classifier Resolution and Feature Pre-Processing

On the basis of the extracted features, a suitable classifier wishes to be selected or developed. A heavy pile of digital images for the classifier's coaching is preferred and some salient parameters of the chosen classifier are obtained, that can be exploited for this classification.

Classification

A classifier distinguishes any given image and categorizes it into two classes: actual and tampered digital image. On the basis of extracting features set, an appropriate classifier is further chosen or planned.

Post-processing

This last step involves morphological operations, which are borne out with the aim to lower false advantageous rate. To discriminate a variety of copy-move patches, matching patches belonging to equal shift vectors are marked to by using the equal color, generally white, to visually locate the duplicated parts.

LITERATURE REVIEW

Today, nevertheless, effective digital picture modifying software makes picture changes straightforward. [1] Guohui Li, et al. proposed DWT, and the SVD which is utilized to the fixed sized overlapping blocks of low frequency in the wavelet sub band. [2] J. Fridrich, et al., detected the copy move forgery and describes an environment friendly and reliable detection method. [3] Babak Mahdian, et al., proposed a method to mechanically become aware of and localize duplicated regions in digital photos.[4] Weiqi Luo, et al., describe an efficient and sturdy algorithm for finding and localizing Region duplication forgery of malicious tampering. [5] A. Thakur, et al. they offered a novel copy, move forgery detection scheme using color illumination, block and key point based. The proposed scheme integrates each block primarily based and key factor based forgery detection methods. [6] Sevinc Bayram, et al., advocates new schemes which use DCT coefficients and Eigen values as features. [7] Z. Lin, et al., detected tampered pictures with the aid of analyzing the double quantization impact hidden amongst the discrete cosine seriously change (DCT) coefficients. [8] M. K. Bashar, Member, et al., advice a duplication detection strategy that can take on two strong elements based on discrete wavelet seriously change (DWT) and kernel primary aspect analysis (KPCA). [10] M. Ghorbani, et al., proposed an improved technique using DWT and Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD) to realize such cloning forgery. [11] Judith A. Redi, et al., described a future assignment for Digital photo Forensics is the extension to different media, and in specific to video. [12] G. Muhammad, et al., proposes a blind reproduction go image forgery detection technique based on DyW. [13] Y. Huang, et al., elevated DCT-based technique is built up to realize this unique artifact. DCT is applied to every block to symbolize its features whereas Truncating is employed to determine the dimension of the features. [14] Y. Wang, et al., advocates a wavelet-based method to notice region duplication forgery. [15] H. C. Nguyen, et al., suggests a method in the first place based on the Radon seriously change and segment correlation in order to enhance the robustness in forgery detection. [16] Gajanan K. Birajdar, et al., presents references on blind techniques for photograph forgery detection. [17] M. A. Sekeh, et al., suggests a superior duplicated location detection mannequin by using the sequential block clustering. This substantially improves the time complexity. [18] Dijana Tralic, et al., developed new database for a CMFD that consist of 260 forged photograph sets. Every image set includes solid image, two masks and authentic picture. Icons are grouped in 5 categories according to applied manipulation: translation, rotation, scaling, mixture and distortion. [19] Tiago Jose de Carvalho, et al. put in a new technique for detecting cast images of people using the lighted color. They urge a novel algorithm based on side factors and the HOG. [20] Ainuddin Wahid Abdul Wahab, et al. concludes that research on the function of the passive method for video forgery detection exist between the semantics of digital information and the authenticity of digital evidence. [21] Mohd Dilshad Ansari, et al. explained that algorithms are now not fantastic in phrases of detecting actual forged region. On the other hand, some algorithms have a very high time complexity. [22] Xiu-Li Bi, et al. proposes an adaptive over-division method for CMF detection. The labeled characteristic points are treated and the morphological operation is given to generate the detected forgery regions. [23] Xiaoyu Chu, et al. evaluates the effectiveness of an anti-forensic attack. [24] SAH Tabatabaei, et al. proposed a system which is made based on an aggregate of hard and gentle authentication using two existing customary approximate message authentication codes (AMACs). [25] Edoardo Ardiz one, et al. proposed that objects are modeled as a circle of connected triangles constructed onto these points. Triangles are matched in accordance to their shapes (inner angles), their content (color information), and the neighborhood function vectors extracted onto the peaks of the triangles. [26] Chi-Man Pun, et al. proposed a system which integrates both blocks based and key point based forgery detection methods. [27] Davide Cozzolino, et al. proposed Dense-field strategies, warranty an optimum performance with recognize to their key stage-based counterparts, at the price of a a good deal greater processing time. [28] Tiago Carvalho, et al. combine statistical telltales provided by using different image descriptors that explore color, form, and texture features. Focus on detecting photo forgeries containing human beings and current a technique for finding the forgery, specifically, the face of a man or a womanhood in an icon. [29] M. Zandi, et al. proposed a CMFD technique that can accurately localize duplicated areas with a life like computational cost. [31] Suvarna G, et al. proposed a heavy direction to realize replica cross forgery, basically involved with duplicating one area in an photo via pasting certain portion of the equal picture on it. [32] Anuja Dixit et al. explained that the picture is split into blocks, and then function vectors are extracted corresponding to exclusive blocks of icons. Screening methods are used to find similarities between blocks.

Today, nevertheless, effective digital picture modifying software makes picture changes straightforward. [26] Chi-Man Pun, et al. offered a novel copy move forgery detection scheme the use of adaptive over segmentation and function factor matching. The proposed scheme integrates each block primarily based and key factor based forgery detection methods. The main contribution of this paper is to (1) design hybrid image forgery detection method using color illumination, color segmentation map and feature detection technique for copy move forgery detection. (2) Ameliorating the performance of a hybrid photograph forgery detection method [5] A. Thakur, by way of Increasing of Precision and Recall the use of coloration illumination and SVM classifier.

The central declaration of problem primarily based on recognizing research gaps is: To learn about the literature survey of the block based and key factor based image forgery detection techniques. Implement hybrid image forgery detection technique using Adaptive method. To study the applied technique with the current techniques based totally on parameters Precision and Recall. Block-based algorithms are computationally luxurious as nicely as inclined to geometrical attacks like rotation, scaling and transformation. Key point based systems are computing environment friendly and invariant to the geometrical transformations, however go through from lower recall rate. Hence, the adaptive hybrid method is developed to master all these defects.

PROPOSED ALGORITHM

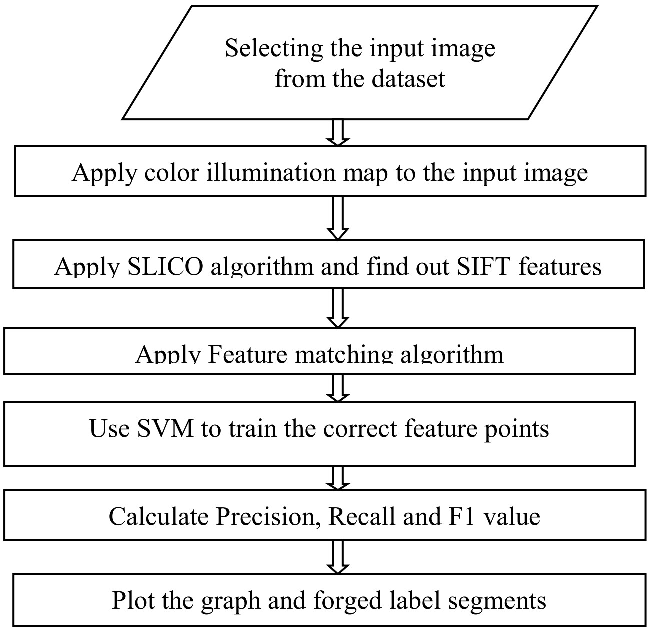
Selecting the input image from the dataset
Apply color illumination map to the input image
Apply SLICO algorithm and find out SIFT features
Apply Feature matching algorithm
Use SVM to train the correct feature points
Calculate Precision, Recall and F1 value
Plot the graph and forged label segments

Figure 1: The proposed algorithm of Copy Move Forgery Detection flowchart.

The idea for developing this algorithm is taken from [5, 26]

Choosing the Dataset

In this block we choose input image from the database [22]. In this database 48 images are present with different size and forged image results are also given to compare the obtained results.

Selecting the Input Image from the Dataset

In this block we have created train and test folder in the working directory of Matlab. We have used SVM to train and test our proposed system. While taking input from database we have to select input image manually so that we can choose correct one from the data base.

Illuminants for Detecting Forgeries

In this step, we incorporated color illuminant maps, to propose a new hybrid technique for selecting visual properties for the detection of image forgeries. We conglomerate color, shape, and texture features in this step. The objective here is to detect inconsistencies in the estimated light source color from the image. The copy move forgery detection process is very time engulfing and erroneous. Our approach is the detection of multiple copy paste block of the image. For the detection of inconsistencies following steps are performed: Figure1 shows that the algorithm SVM train and test database in which algorithms estimating a color space of the input image, images are segmented into same object color, and extracting image visual cues (e.g., color, texture, and shape), information into feature vectors. SVM incorporate image feature vectors to learn intra and inter class patterns of the images to classify each new image feature vector. We have to select those super pixels for the detection of forgery portion using block feature extraction SLIC algorithm and estimate illuminant color. Furthermore we have to calculate the distance from the selected super pixels to the other ones generating a distance map uing block feature matching algorithm. Eventually the forgery detection decision is taken automatically with the help of machine learning techniques such as SVM classifiers. Using morphological operation, we discarded isolated pixels, leaving only boundary pixels and generating segmented forgery area.

As we have undergone the research and study of different papers on image forgery detection and find out color space is not incorporated for the detection of image forgery. We propose to augment the number of explored color spaces in order to capture the smallest nuances present in such maps not visible in the original representation of a transformed image to an illuminant map representation. We consider the Lab, HSV, and original normalized RGB color spaces [21]. We have chosen such color spaces, which are popular choices in image processing literature [20]. It has subsequently inspired the further design of statistical descriptors for color constancy. We followed the extension of this idea, the generalized gray world approach by van de Weijer algorithm 1 Illuminants for detecting forgeries.

Simple Linear Iterative Clustering (SLICO) Algorithm

With the help of SLICO algorithm the entire image is ramified into smaller blocks. SLICO is used to generate super pixels starting from a signal of length N. In this algorithm input image is segregated into several non-overlapping regions of irregular shape, as shown in Fig. 6. Forgery regions detection algorithm is incorporated for the matching of those non-overlapping and irregular regions. Simple linear iterative clustering (SLICO) algorithm is incorporated for the generation and enumeration of non-overlapping and irregular shape super pixels for the image, as individual blocks. K-means clustering approach is incorporated for the generation and enumeration of the super pixels and it detect edges and boundaries very easily and correctly.

SLICO is incorporated for decrementing execution expenses, irregular and non-overlapping block give better results than regular block size. It is highly perplex and intricate to calculate the initial size of the super pixel. SLICO select maximum value of color distance.

Scale-Invariant Feature Transform (SIFT) Algorithm

SIFT frames and their descriptors is calculated using SIFT algorithm. Proposed algorithm divide the input image into blocks with adaptive initial sizes. Adaptive size of the block increases the accuracy of the forgery detection results. Proposed algorithm gives good detection results and reduces computational expenses. Block features are generated from Image blocks. In past most of the methods used regular block size and features are calculated from these blocks; however, those features are not able to provide location information. In this paper we have used hybrid technique to detect feature points from all image blocks and these are not affected by transformational attacks. SIFT is key point based copy move forgery detection method, which is used to find out feature points.

Block Feature Matching Algorithm

Here in this algorithm block features are matched with other blocks for enumerating the correct matches between each block. Existing methods detect specific block pair only if other blocks are also matched by considering that they have the same shift vector. Threshold is defined by user and if the shift vector exceeds that threshold, then shift vector are identified as forged region. In our algorithm, we match patches using shift vector threshold, if pixel value is less than 0.15 that pixel value is considered and if the pixel distance is greater than 0.15 then that pixel value is non considerable. Two patches are created A, B and key points are calculated as x, y respectively. With the help of threshold value algorithm provide decision about correct key point. Using color grow algorithm highlight the detected key points. Morphological operation is incorporated to facilitate proper shape of forged block. In this step human intervention is needed. With the help of SVM we reduce human intervention. SVM is used to train proposed system and give correct forgery detection results.

Forgery Region Extraction Algorithm

Detected feature points present idea about location of forged portion. Super pixels locate image forgery locations and segment the host image very well. With the help of SIFT, we get labeled feature points and these are replenished with small super pixels to obtain the forged regions. By the incorporation of morphological operation we detect correct forged portion of the image. SVM train the system and generate correct forgery regions without any human intervention.

We have performed experiment to find out precision, recall and f1 value of 48 PNG high resolution plane copy move forged images and find out image forgery detection at image level with Precision=97.20%; Recall=100% and F1=98.3%.

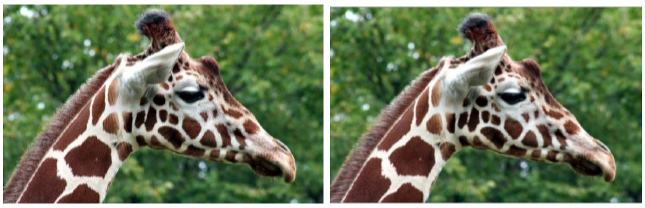

Figure 2: (a) Input forged Image, (b) Smooth image

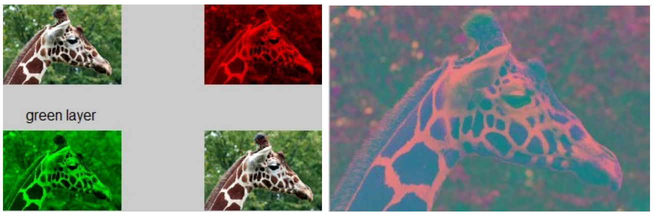

Figure 3: (a) Fabric image with Red, Green and Blue color map, (b) Color converted image.

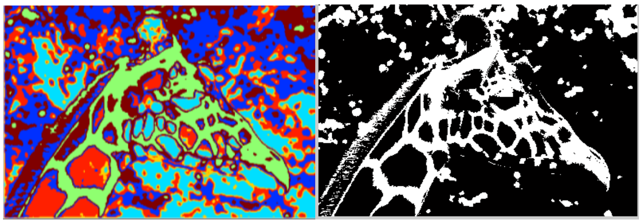

Figure 4: (a) Segmentation map, (b) color image to BW with 0.5 intensity of BW color

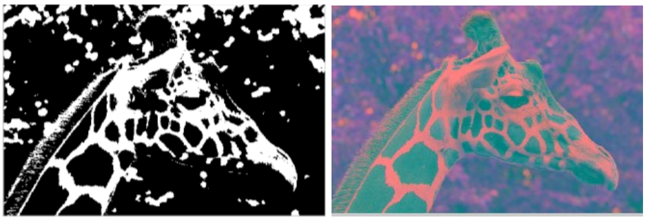

Figure 5: (a) Morphological operation to clean image, (b) Color to perform SLICO operation

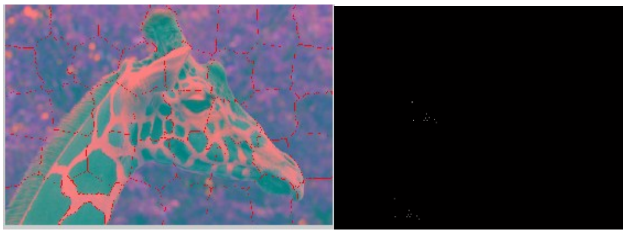

Figure 6: (a) SLICO operation, (b) Key point or Pixel generation

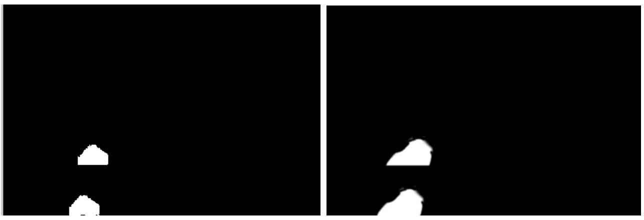

Figure 7: (a) Final Forged Regions, (b) Ground truth image

The approach integrates both block and key point based forgery detection techniques. This approach exploits the capacity of coloration segmentation, segmentation map, SLICO, SIFT and SVM to detect comparable regions in a tampered image. It consists of exclusive stages: coloration photo segmentation, characteristic extraction and description, patch function matching, shade illuminated key point matching and color illuminated forgery vicinity extraction. The following sections current exact description of each phase.

EXPERIMENTAL WORK AND RESULTS

The experimental results are shown in table 1 with different block size of the image for different parameters. The Precision and recall values are calculated using:

$$Precision = \frac{\text{correctly detected forged pixels}}{\text{number of totally detected forged pixels}} \quad (1)$$

$$\text{Recall} = \frac{\text{correctly detected forged pixels}}{\text{number of forged pixels}} \qquad (2)$$

Table1: Comparison of proposed algorithm with different block size.

Host Image:I1	S=150	S=250	S_I1=199	Adaptive	Proposed
Precision	91.44	91.91	93.85	95.52	95.55
Recall	69.99	69.74	99.12	99.25	99.75
Host Image:I2	S=150	S=250	S_I2=159;	Adaptive	Proposed
Precision	93.07	93.26	96.6	97.82	97.89
Recall	90.75	77.43	78.9	85.12	86.75
Host Image:I3	S=150	S=250	S_I3=224	Adaptive	Proposed
Precision	96.9	95.59	95.28	96.14	97.95
Recall	81.49	89.46	95.19	97.82	98.55

The experimental results show comparison with state of the art technique in table 2 with different parameters. The F1 value is calculated using:

F1= (Recall × Precision) / (Recall × Precision) (3)

Table 2: Comparison of proposed algorithm with state of the art techniques.

COPY-MOVE IMAGE FORGERY DETECTION AT IMAGE LEVEL			
Host Image:I1	**Precision**	**Recall**	**F1**
Bravo [13]	87.27	100	93.2
Wang [8,9]	92.31	100	96
SIFT [15, 16]	88.37	79.17	83.52
SURF [17, 19]	90.49	89.58	90.53
Pun [2] Fixed	95.92	97.92	96.91
Pun [2] Adaptive	96	100	97.96
A Thakur [1]	97.25	100	98.53
Proposed	98	100	99

The proposed algorithm is compared in table 2 with other methods. The average precision is 98%, recall is 100% and F1 is 99% is achieved. This experiment is performed on 48 high resolution images. These images are of different categories like natural, animals, buildings etc.

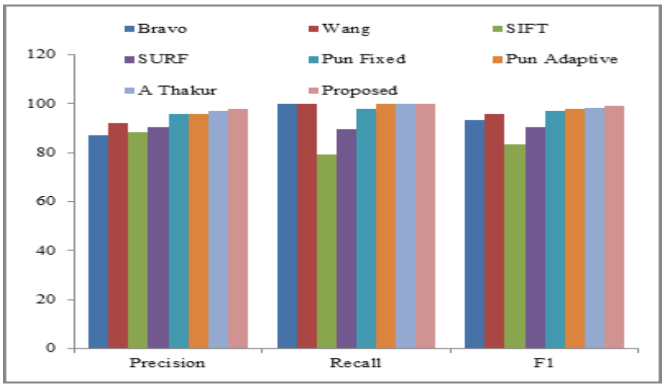

Figure 8: Bar graph of Precision, Recall and F1 values comparison of proposed algorithm with others.

Table 3: Comparison of precision value between proposed algorithm and others algorithms for JPEG compression attack.

PRECISION

	SIFT	**SURF**	**Circle**	**RSIFT**	**Bravo**	**Pun**	**AT**	**Prop.**
100	0.45	0.56	0.66	0.77	0.85	0.85	0.89	0.9
90	0.47	0.51	0.59	0.78	0.69	0.8	0.82	0.85
80	0.46	0.5	0.45	0.78	0.42	0.8	0.86	0.82
70	0.45	0.5	0.38	0.7	0.39	0.73	0.73	0.71
60	0.44	0.51	0.25	0.7	0.26	0.72	0.75	0.76
50	0.45	0.5	0.13	0.72	0.25	0.72	0.74	0.77
40	0.47	0.47	0.12	0.65	0.2	0.71	0.61	0.65
30	0.46	0.5	0.11	0.61	0.12	0.61	0.5	0.58
20	0.45	0.48	0.1	0.41	0.11	0.45	0.4	0.46

The proposed algorithm is compared in table 3 with other algorithms for precision. This comparison is performed for JPEG compressed images precision value. The average precision is 72% is achieved. This experiment is performed on 48 high resolution JPEG compressed images. These images are compressed with factor of -10 from 100 to 20.

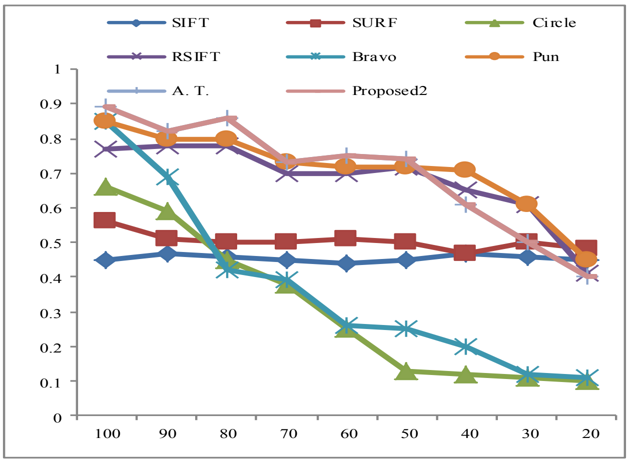

Figure 9: Pixel level forgery detection results Avg. Precision = 72% for JPEG compression at 100 to 20, in steps of −10.

Table 4: Comparison of recall value between proposed algorithm and others algorithms for JPEG compression attack.

RECALL

	SIFT	**SURF**	**Circle**	**RSIFT**	**Bravo**	**Pun**	**AT**	**Proposed**
100	0.55	0.6	0.25	0.55	0.25	0.71	0.7	0.75
90	0.54	0.54	0.1	0.6	0.09	0.68	0.59	0.6
80	0.54	0.56	0.08	0.56	0.05	0.7	0.68	0.65
70	0.53	0.55	0.07	0.51	0.04	0.62	0.66	0.62
60	0.52	0.56	0.02	0.5	0.02	0.58	0.59	0.63
50	0.53	0.55	0.01	0.5	0.01	0.6	0.68	0.7
40	0.54	0.48	0.01	0.43	0.01	0.58	0.59	0.6
30	0.49	0.49	0.01	0.42	0.01	0.45	0.5	0.55
20	0.39	0.47	0.01	0.18	0.01	0.25	0.4	0.45

The proposed algorithm is compared in table 4 with other algorithms for recall. This comparison is performed for JPEG compressed images recall value. The average recall is 62% is achieved. This experiment is performed on 48 high resolution JPEG compressed images. These images are compressed with factor of 10 from 100 to 20.

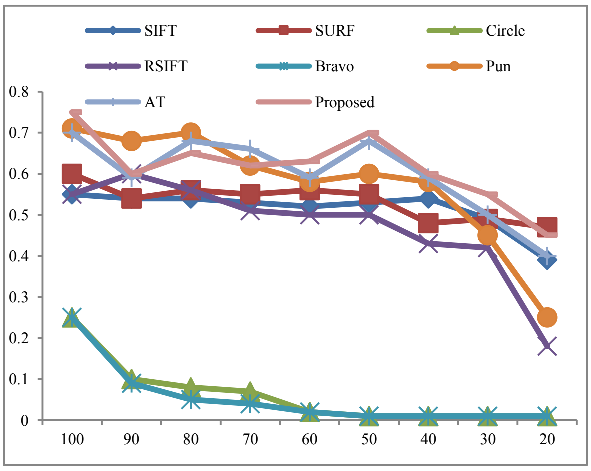

Figure 10: Pixel level forgery detection Recall = 61% for JPEG compression at 100 to 20, in steps of −10.

Table 5: Comparison of F1 value between proposed algorithms with different block size for JPEG compression attack.

F1

	SIFT	SURF	Circle	RSIFT	Bravo	Pun	AT	Proposed
100	0.5	0.59	0.35	0.63	0.39	0.78	0.72	0.75
90	0.5	0.51	0.19	0.69	0.16	0.74	0.7	0.73
80	0.51	0.51	0.11	0.63	0.07	0.75	0.78	0.8
70	0.5	0.52	0.11	0.6	0.06	0.69	0.68	0.7
60	0.48	0.53	0.04	0.59	0.05	0.64	0.65	0.68
50	0.49	0.52	0.03	0.56	0.04	0.66	0.69	0.65
40	0.5	0.48	0.02	0.55	0.03	0.62	0.7	0.75
30	0.48	0.49	0.03	0.5	0.02	0.52	0.51	0.55
20	0.4	0.47	0.03	0.2	0.03	0.32	0.4	0.45

The proposed algorithm is compared in table 5 with other algorithms for F1 value. This comparison is performed for JPEG compressed images F1 value. The average recall is 67% is achieved. This experiment is performed on 48 high resolution JPEG compressed images. These images are compressed with factor of -10from 100 to 20.

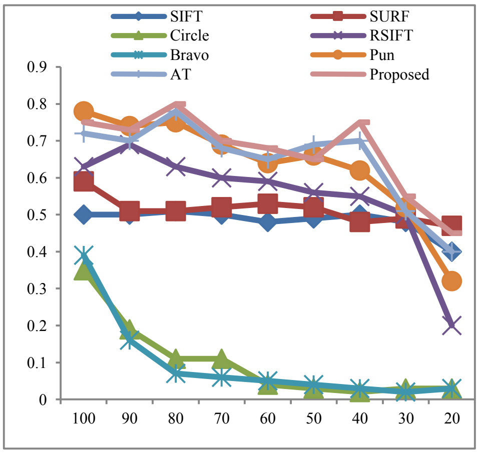

Figure 11: Pixel level forgery detection results F1 = 67% for JPEG compression at 100 to 20, in steps of −10.

In this paper numerous experiments are carried out to discover out precision, recall and f1 cost of 48 high resolution .png copy move forged photographs and discover out picture forgery detection at pixel level with Precision=72%; Recall=62% and F1=61%.

CONCLUSION

In this paper numerous experiments are performed to discover out precision, recall and f1 value of 48 .png high resolution images. Copy move forged image detection at image level achieved average precision 98%, recall 100% and f1 99%. The total forged images with JPEG compression are 432. For the jpeg attack all images are compressed with a factor of -10. The achieved average accuracy for precision is 72%, recall is 62% and F1 is 61% for jpeg compressed images. These results are compared with state of the art techniques. The proposed results give better copy move forgery detection with or without attacks.

REFERENCES

[1] Guohui Li, Qiong Wu, Dan Tu, Shaoie Sun, "A Sorted Neighborhood Approach For Detecting Duplicated Regions In Image Forgeries Based On Dwt And Svd", IEEE Signal Processing Magazine, pp: 25-37.

[2] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images, " in Proc. of the Digital Forensic Research Workshop, Cleveland, OH, pp. 55–61, 2003.

[3] Babak Mahdian, StanislavSaic, "Detection of copy move forgery using a method based on blur moment invariants", Elsevier, 2006

[4] WeiqiLuo, Jiwu Huang, "Robust Detection of Region Duplication Forgery in Digital Image", The 18th International Conferenceon Pattern Recognition (ICPR'06).

[5] Thakur, A. & Jindal, N. Multimed Tools Appl (2018). https://doi.org/10.1007/s11042-018-5836-5.

[6] SevincBayram, HusrevTahaSencar, NasirMemon, "An Efficient and Robust Method for Detecting Copy Move Forgery", IEEE International Conference on Acoustics, Speech and Signal Processing, 2009. ICASSP 2009, DOI: 10.1109/ICASSP.2009.4959768

[7] Zhouchen Lin, Junfeng He, Xiaoou Tang, Chi-Keung Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis", Pattern Recognition, doi: 10.1016/j.patcog.2009.03.019, 2009.

[8] M.K.Bashar, K.Noda, N.Ohnishi, and K.Mori, "Exploring Duplicated Regions in Natural Images", IEEE. vol. PP no. 99, 25 March 2010

[9] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, "Exploring duplicated regions in natural images, "IEEE Transactions on Image Processing, 2010.

[10] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy move image forgery detection, "in Proc. of the 18th International Conference on Systems, Signals and Image Processing, pp. 1–4, 2011.

[11] Judith A.Redi&WiemTaktak& Jean-LucDugelay, "Digital image forensics: a booklet for beginners", Multi med Tools Appl (2011), Springer, 51:133–162, DOI10.1007/s11042-010-0620-1.

[12] G. Muhammad, M. Hussain, K. Khawaji, and G. Bebis, "Blind copy move image forgery detection using dyadicun decimated wavelet transform, " in Proc. of the 17th International Conference on Digital Signal Processing, pp. 1–6, 2011.

[13] Yanping Huang, Wei Lu, Wei Sun, Dongyang Long, "Improved DCT-based detection of copy-move forgery in images", Forensic Science International 206, 178–184, 2011.

[14] Y. Wang, K. Gurule, J. Wise, and J. Zheng, "Wavelet based region duplication forgery detection, "in Proc. of the 9th International Conferenceon Information Technology, pp. 30–35, 2012.

[15] H. C. Nguyen, and S. Katzenbeisser, "Detection of copy-move forgery in digital images using rad on transformation and phase correlation," in Proc. of the 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 134–137, 2012.

[16] Gajanan K. Birajdara, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey", Elsevier, vol. 10, no. 3, October 2013, Pages 226-245, DOI: 10.1016/j.diin.2013.04.007.

[17] M. A. Sekeh, M. A. Maarof, M. F. Rohani, and B. Mahdian, "Efficient image duplicated region detection model using sequential block clustering, "Digital Investigation, vol. 10, no. 1, pp. 73–84, 2013.

[18] DijanaTralic, Ivan Zupancic, Sonja Grgic, MislavGrgic, "CoMoFoD - New Database for Copy Move Forgery Detection", 55th International Symposium ELMAR-2013, 25-27 September 2013, Zadar, Croatia.

[19] Tiago JosedeCarvalho, Christian Riess, Elli Angelopoulou, HélioPedrini, and Anderson de Rezende Rocha," Exposing Digital Image Forgeries by Illumination Color Classification", Ieee Transactions On Information Forensics And Security, vol. 8, no. 7, 2013.

[20] Ainuddin Wahid Abdul Wahab, Mustapha AminuBagiwa, MohdYamanidnadris, Suleman Khan, ZaidiRazak, "Passive Video Forgery Detection Techniques: ASurvey", IEEE International Conferenceon Information Assurance and Security (lAS), 2014.

[21] Mohd Dilshad Ansari, S.P.Ghrera&VipinTyagi, "Pixel-Based Image Forgery Detection:A Review", IETE Journal of Education, vol. 55, no 1, 2014.

[22] Xiu-Li Bi, Chi-Man Pun, and Xiao-Chen Yuan, "Over-Segmentation Image Forgery Detection," inProceedings of International Conference on Electronics and Automation Control, 2015.

[23] Xiaoyu Chu, Matthew Christopher Stamm, Yan Chen, and K. J. Ray Liu, "On AntiforensicConcealability With Rate-Distortion Tradeoff", IEEE TRANSACTIONS ON IMAGE PROCESSING, Vol. 24, No. 3, MARCH 2015

[24] Seyed Amir HosseinTabatabaei, Obaid Ur-Rehman, NatasaZivic, and ChristophRuland, "Secure and Robust Two-Phase Image Authentication", IEEE Transactions On Multimedia, Vol. 17, No. 7, July 2015

[25] EdoardoArdizzone, Alessandro Bruno, and Giuseppe Mazzola, "Copy–Move Forgery Detection by Matching Triangles of Keypoints", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 10, October 2015

[26] ChiMan Pun, Xiao-ChenYuan, and Xiu-LiBi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching", IEEE Transactions On Information Forensics and Security, Vol. 10, No. 8, August 2015.

[27] DavideCozzolino, Giovanni Poggi, and Luisa Verdoliva, "Efficient Dense-Field Copy–Move Forgery Detection", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 11, November 2015

[28] Tiago Carvalho, Fábio A. Faria, HélioPedrini, Ricardo da S. Torres, and Anderson Rocha, "Illuminant-Based Transformed Spaces for Image Forensics", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 4, April 2016

[29] Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, and AlirezaTalebpour, "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 11, November 2016

[30] Dhania V S, Harish Binu K P, "Exposing Digital Image Forgeries Using Feature Extraction and Adaptive Over Segmentation", International Journal of Innovative Researchin Science, Engineering and Technology, vol. 5, no. 8, August 2016

[31] Suvarna G. Upase, Sunil V. Kuntawar, "Copy Move Detection of Image Forgery by using DWT and SIFT Methodologies", International Journal of Computer Applications, vol. 148, no. 7, August 2016. Anuja Dixit and R. K. Gupta, "Copy-Move Image Forgery Detection using Frequency- based Techniques: A Review", International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 9, no. 3, pp. 71-88, 2016.